Секция 05. Технические науки Секция

**Кибербезопасность: как защитить личные данные в сети**

Саров Руслан Ибрагимович

ГБОУ РО “РКРПТ”

Первый курс ВЕБ-12к

Костыльга Анна Григорьевна

**Содержание**

1. Введение
2. Кто такой специалист по кибербезопасности и что он должен делать?
3. Участвует в разработке по кибербезопасности.
4. Борется с фишингом.
5. Заключение.

**Введение**

Грамотный подход к кибербезопасности предполагает несколько уровней защиты для компьютеров, сетей, программ и данных. Организация должна наладить правильное взаимодействие людей, процессов и технологий для развертывания эффективной защиты от кибератак. Система унифицированного управление угрозами (UTM) автоматизирует интеграцию ряда продуктов Cisco для обеспечения безопасности и ускоряет реализацию ключевых функций защиты: обнаружения, анализа и устранения.

Пользователи должны понимать и соблюдать базовые принципы защиты данных, такие как выбор надежных паролей, осторожность при обращении с вложениями в электронной почте и резервирование данных.

Организации должны развернуть систему по предотвращению кибератак и устранению их последствий. В этом может помочь одна признанная стратегия. Она объясняет, как выявлять атаки, защищать системы, обнаруживать угрозы, реагировать на них и устранять последствия успешных атак. Смотреть видео с описанием стратегии NIST CyberSecurity

Технологии лежат в основе создания средств компьютерной безопасности для защиты организаций и частных лиц от кибератак. Защищать нужно объекты трех основных групп: конечные устройства, такие как компьютеры, интеллектуальные устройства и маршрутизаторы, сети и облако. Распространенными технологическими решениями для защиты этих объектов являются межсетевые экраны нового поколения, фильтрация DNS, защита от вредоносного ПО, антивирусное ПО и решения для защиты электронной почты.

Передовыми программами кибербезопасности в современном сетевом мире пользуется каждый. На индивидуальном уровне кибератака может привести к самым разным последствиям: от кражи личности до попыток вымогательства и потери таких важных данных, как семейные фотографии. Любой человек зависит от объектов критически важной инфраструктуры: электростанций, больниц и финансовых учреждений. Защита этих и других организаций имеет принципиальное значение для нормального функционирования нашего общества.

Все люди также пользуются результатами трудов исследователей в области кибербезопасности. К таким исследователям относятся 250 ученых из команды Talos, которые изучают новые угрозы и подходы к кибератакам. Они выявляют уязвимости, рассказывают широкой аудитории о важности кибербезопасности и усиливают защиту средств с открытым исходным кодом. Их работа делает Интернет безопаснее для всех.

## **Кто такой специалист по кибербезопасности и что он должен знать?**

Сложности начинаются уже здесь. Если говорить коротко, специалист по безопасности – это тот, кто очень хорошо разбирается в технологиях и людях. Стеки технологий здесь не будем указывать, они сильно разнятся от направления к направлению. В целом специалисту по безопасности нужны базовые знания и навыки в следующих сферах:

* разработка и тестирование. Безопаснику, который работает в команде разработки, предстоит находить ошибки и исправлять их. Не все ошибки, разумеется, а того характера, которые влияют на устойчивость системы;
* построение архитектуры. Специалист по кибербезопасности – один из тех, кто выдвигает требования к архитектуре будущего продукта и следит за их выполнением;
* управление рисками. Мало просто знать IT, нужно понимать, какие риски будут возникать при использовании конкретной технологии конечным потребителем;
* психология. Далеко не всегда люди обращаются с данными так, как хотелось бы безопаснику. Более того – люди разные. По культуре, образованию, да банально – по возрасту. Нужно не только знать типичное поведение разных групп клиентов, но и суметь предугадать их поведение в определённой ситуации. Речь идёт как о внешних клиентах, так и о внутренних, то есть о сотрудниках. А ещё этих людей нужно убедить обращаться со своими данным в соответствии с требуемым уровнем безопасности;
* правовая база. О какой именно базе идёт речь – зависит от специализации. Например, тем, кто борется с интернет-фишингом, нужно знать, в каком случае и как можно принудительно закрыть мошеннический сайт.

**Кибербезопасник** – это и айтишник, и разработчик, и тестировщик, и риск-менеджер, и психолог, и юрист, и человек, который может рассказать понятным языком о каждой из этих областей знания. Это определение содержит значительную часть ответа на вопрос «Почему таких специалистов остро не хватает?» Потому что найти человека, который разбирается во всём этом, очень сложно.

**Участвует в разработке продуктов и тестировании**

Эксперт по кибербезопасности входит в каждую продуктовую команду. Понятно, что продукты делают люди, а людям свойственно совершать ошибки. Задача эксперта эти ошибки находить и учить людей, чтобы они как минимум не повторялись. Безопасник практически живёт в команде разработки, без его участия не происходит ни один этап – от планирования архитектуры до релиза.

Специалист формулирует требования, контролирует их исполнение, анализирует риски, проходит приёмо-сдаточные испытания, анализирует код и помогает исправить баги. Так каждый наш продукт становится безопасным. Не на 100% (таких не бывает), но на максимально близкое к этому значение.

**Участвует в тестировании**

Есть внешние и внутренние тестирования.

Внутренние – своего рода «казаки-разбойники» для команды. Есть «злоумышленники», которые, зная внутренности системы, пытаются её взломать, и есть «безопасники», которым нужно сохранить систему в целости и вычислить хакера. И это не только про поиск слабых мест, но ещё и про тренировку команды.

Есть также практика, когда не сама команда разработки делится на «красных» и «синих», а приглашается сторонняя организация. Её специалисты пытаются проникнуть внутрь системы. У нас такой организацией является BI.ZONE – дочерняя компания Сбера. С её помощью легко понять, насколько защищён внешний периметр любого сервиса и отдельной структуры бизнеса.

В большинстве случаев о таких тестированиях заранее известно. И тестировщики, что логично, никогда не доходят до конца. Они находят уязвимость и показывают её – на этом тестирование заканчивается.

**Борется с фишингом**

В период пандемии Россия вышла на первое место в мире по размещению фишинговых ресурсов и вредоносным рассылкам. За первые шесть месяцев 2021 года предотвращено более 36 млн попыток перехода российских пользователей на различные фишинговые сайты, из них более 300 тысяч попыток перехода пользователей на страницы, мимикрирующие под наиболее крупные финансовые организации.

С этими сайтами идёт работа, в том числе по разделегированию доменных имён. Кстати, фишинговыми ресурсами в том числе занимается BI.ZONE. Однако сколько бы мы ни старались, работа не прекращается: мы закрываем сайты, мошенники создают новые.

Отдельная история – мошенничество по телефону. За первое полугодие 2021-го 57% россиян получали звонки от телефонных мошенников. Каждый десятый россиянин понёс финансовый ущерб. Бороться с телефонным мошенничеством крайне сложно, и ключевая часть работы – обучение клиентов.

Бывает и так, что мошенником действительно является сотрудник банка. Никто не застрахован от внутреннего нарушителя.

Поэтому отдельный набор технологий направлен на то, чтобы предотвращать действия таких людей, выявлять их и снижать потенциальный ущерб от их действий. Здесь есть контроль за обращением с данными, контроль сотрудников с привилегированным доступом к информационным системам и ещё ряд мер.

**Заключение**

Киберпреступность сегодня составляет значительно более серьезную опасность, чем 5 лет назад, в связи с использованием преступниками новейших информационных технологий, а также через растущую уязвимость современного индустриального общества.

Невзирая на усилия государств, которые направлены на борьбу с киберпреступниками, их количество в мире не уменьшается, а, напротив, постоянно растет.

Ни одно государство сегодня не способно противостоять этому злу самостоятельно. Неотложной является потребность активизации международного сотрудничества, для которого является актуальным, в частности, налаживание международно-правового механизма регуляции.

Но ввиду того, что в современных условиях значительная часть средств борьбы с киберпреступлениями, как и с другими преступлениями международного характера, принадлежит к внутренней компетенции каждого отдельного государства, необходимо параллельно развивать и национальное законодательство, направленное на борьбу с компьютерными преступлениями, согласовывая его с международными нормами права и опираясь на существующий позитивный опыт.

И подводя итоги, хочется сказать, что есть разные типы хакеров: и те, у кого есть совесть и мирные принципы и те, кому заработать 1млн долларов на нашей невнимательности – это норма. Поэтому я бы хотел, чтобы вы стали более внимательными и подготовленными в сфере кибербезопасности. Человек все еще остается самым слабым звеном защиты. Он может быть в плохом настроении, быть усталым, да и в целом есть угрозы, от которых нельзя полностью защититься.

Таким образом, можно считать, что поставленные цели достигнуты. Мы узнали много нового, интересного и полезного. Полученные знания пригодятся в жизни всем нам.

Чем сильнее становится зависимость жизни общества от компьютерных систем, тем опаснее уязвимость России и других стран от всевозможных мастей киберпреступников. О безопасности надо думать сегодня, завтра уже может быть поздно.

**Список используемых источников**

1. [Cisco](https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html)
2. [Kaspersky](https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security)
3. [Habr Blog Sber](https://habr.com/ru/company/sberbank/blog/592275/)